



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 31, 2022

VIA E-Mail

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent The Salvation Army, a Georgia corporation for the Potomac Division (“TSA”) located at 2626 Pennsylvania Avenue, NW Washington, DC 20037, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, TSA does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about June 6, 2022, TSA learned that a recently separated temporary employee directed certain emails from the individual’s TSA email account to a personal email account. Upon learning of the incident, TSA quickly launched an investigation to determine its nature and scope. Through the investigation, TSA determined that the former employee Blind Carbon Copied limited messages and attachments from the individual’s TSA email account to a personal email account during the course of the individual’s employment. TSA conducted a thorough and comprehensive review of the copied messages and attachments and determined limited sensitive information was contained in the emails. This review was recently completed. TSA also reached out to the individual regarding the emails.

The information that could have been subject to unauthorized access includes name, address, and financial account information.

Mullen.law

Notice to Maryland Resident

On or about August 31, 2022, TSA provided written notice of this incident to one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, TSA moved quickly to investigate and respond to the incident, review the at issue emails for sensitive information, and identify potentially affected individuals. Further, TSA notified local law enforcement regarding the incident. TSA is also working to implement additional safeguards and training to its employees to prevent similar incidents in the future. TSA is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, TSA is providing impacted individuals with guidance on how to better protect against identity theft and fraud. TSA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. TSA is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/dle
Enclosure

EXHIBIT A

<<Insert TSA Potomac Division Letterhead>>

<<Return Mail Address>>

SAMPLE A SAMPLE

ADDRESS 1

ADDRESS 2

<<Date>>

Dear Sample A. Sample,

The Salvation Army, a Georgia corporation for the Potomac Division (“TSA”) is writing regarding a recent incident that may affect the security of some of your information. This notice provides additional information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? TSA recently learned that a former temporary employee directed certain emails from her TSA email account to a personal email account. Upon learning of the incident, we quickly launched an investigation to determine its nature and scope. We also notified local law enforcement of this incident. Through the investigation, we determined that the former employee Blind Carbon Copied limited messages and attachments from the individual’s TSA email account to a personal email account during the course of the individual’s employment with TSA. We conducted a thorough and comprehensive review of the copied messages and attachments for sensitive information, and the review determined that certain information relating to you was in the messages and attachments. TSA also reached out to this individual regarding these emails.

What Information Was Involved? Though our review, we determined that information relating to your loan forgiveness application was present in the copied messages and attachments, including your name, and [data elements]. **Please note we are not aware of any misuse of your personal information related to this event and are sharing this information as part of our valued relationship with you.**

What We Are Doing. We treat our responsibility to safeguard personal information in our possession as an utmost priority. As such, we responded immediately to this incident and has been working diligently to provide you with an accurate and complete notice of the incident as quickly as possible. As part of the ongoing commitment to the privacy and security of information in our care, we are conducting a review of existing internal policies and procedures relating to data protection and security. We are also implementing enhanced employee training protocols to better prevent future incidents. We are providing notice of this incident to the impacted individuals and to state regulators, where required.

As an added precaution, we are offering you complimentary access to 12 months of credit and identity monitoring services through TransUnion. We encourage you to activate these services, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. You may also review the information contained in the attached *Steps You Can Take to Protect Personal Information*. There you will also find more information on the complimentary credit monitoring services we are making available to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call TSA at 404-728-1300 ext. 10032 9am – 5pm ET. We take the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

<<TSA Signatory Signature Image>>

Leon Ferráez, Captain

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Complimentary Credit Monitoring Services

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code **[CM Code]** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **[Call Center TFN]**. When prompted, enter the following 6-digit telephone pass code **[Pass Code]** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain 12 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *myTrueIdentity* online Credit Monitoring service anytime between now and **12/31/2022**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.